

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) An information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2, said information-processing apparatus comprising:

a memory holding a table of candidates of disturbance data XI which maintains maintain a constant Hamming weight before and after processing said disturbance data XI with said predetermined processing OP1;

a selector for selecting ~~said one of said~~ disturbance data XI from said table; a disturbance data processing means for performing said predetermined processing OP1 by using said disturbance data XI selected by said selector in order to generate a disturbance data XO,

a data transform means for transforming said input data D1 by using said disturbance data XI selected by said selector, to generate transformed data H1;

a transformed-data-processing means for performing said predetermined processing OP1 ~~on said input data D1, or a processing different from said predetermined processing OP1~~ on said transformed data H1, in order to generate processed transformed data H2; and

a data inverse-transform means for performing an inverse-transformation processing OP2 on said processed transformed data H2 by using processed

disturbance data XO generated by said disturbance-data-processing means, in order to generate said processed data D2 which can also be obtained without transformations as a result of said predetermined processing OP1 carried out on said input data D1.

2. - 27. (canceled)

28. (currently amended) An information-processing apparatus serving as a data-processing means for carrying out predetermined processing OP1 on input data D1 in order to produce a result of said predetermined processing as processed data D2, said information-processing apparatus comprising:

a memory holding a table of candidate pairs of disturbance data XI and disturbance data XO, wherein said disturbance data XI of said candidate pairs maintains a constant Hamming weight before and after processing said disturbance data XI with said predetermined processing OP1, and wherein said disturbance data XO is obtained from-said processing said disturbance data XI with said predetermined processing OP1,

a selector for selecting-a said pair of disturbance data XI and XO from said table,

a data transform means for transforming said input data D1 by using said disturbance data XI of-a said pair of said disturbance data XI and XO selected by said selector, to generate transformed data H1;

a transformed-data-processing means for performing said predetermined processing OP1 ~~on said input data D1, or a processing different from said~~

predetermined processing OP1 on said transformed data H1, in order to generate processed transformed data H2; and

a data inverse-transform means for performing an inverse-transformation processing OP2 on said processed transformed data H2 by using said disturbance data XO of said selected pair, in order to generate said processed data D2 which can also be obtained without transformations as a result of said predetermined processing OP1 carried out on said input data D1.